UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,747	12/21/1999	XIN WANG	D/99164Q	4043

7590 04/14/2004

Marc S. Kaufman
NIXON PEABODY LLP
8180 Greensboro Drive
McLean, VA 22102

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	16

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/468,747	Applicant(s) WANG, XIN	
	Examiner Jung W Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11 and 12*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 2, and 4-13 have been examined. Applicant amended the Specification and claims 1 and 4 in the amendment filed December 12, 2004 (paper number 13). Applicant further amended claims 1 and 4, canceled claim 3, and added new claims 8-13 in the supplemental amendment filed February 26, 2004 (paper number 14).

Response to Amendment

2. Examiner withdraws the objection to the Specification as the amendment to disclosure filed on December 12, 2003 overcomes the objection.

3. Examiner withdraws the objection to the title as the amended title listed in the amendment filed on December 12, 2003 is more clearly indicative of the claimed inventions.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to

which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claims define a method for protecting a data file on a computer system wherein among other steps, a generation step forms a transformation key from a grantor's decryption key, a grantee's encryption key and other data which is data file independent (see claims 1 and 4). However, the suggested enabling portion of the specification as indicated by the applicant in the supplemental amendment filed on March 29, 2004 (paper number 15) (see paper number 15, page 2, 2nd and 3rd paragraph) is not enabling for the claimed limitation. The two embodiments disclosed in the suggested enabling portion in the specification in regards to the generation of the transformation key (see Specification page 30, lines 10, 20-26 and page 32, lines 26-28) defines the transformation key as being generated from a grantor's decryption key, a grantee's decryption key and other data which is data file independent (specifically a variable g^k or ciphertext s^inv(a) such that g is a generator of a cyclic group, k is a random number, s is the grantor's encryption key to the power of k and inv(a) is the inverse of the grantor's decryption key). As such, the specification is not enabling for the claimed inventions.

6. Claims 1-2 and 4-13 are not rejected over the present prior art, but it is unclear if they are allowable pending clarification over the 35 U.S.C. 112, first paragraph issue as indicated above.

Allowable Subject Matter

The following is a statement of reasons for the indication of allowable subject matter: The amended independent claims define a proxy encryption method, which uses a proxy key to enable transfer of decryption rights of a secured data file wherein transformation is non-commutative and the proxy key is public. These two features in combination distinguish the invention from other proxy encryption schemes known at the time the invention was made, specifically those disclosed by Mambo (see Specification, pages 26-28; see Mambo et al. "Proxy Signatures for Delegating Signing Operation") and Blaze (see Specification, pages 28-30; see Blaze et al. "Divertible Protocols and Atomic Proxy Cryptography"). As defined in the applicant's claims, the proxy key is comprised of a decryption key of a grantor, an encryption key of a grantee and a third variable. Unlike Mambo, which requires that the proxy key is also used to decrypt the transformed encrypted data file, applicant's invention only uses the proxy key in the transformation step to transfer decryption rights of the secured data file: the inclusion of the grantee's encryption key to generate the proxy key of the applicant's invention establishes a condition in the transformation step that only the grantee can decrypt the transformed encrypted data file using her private decryption key; hence, the proxy key need not be a shared secret between the grantor and grantee. Furthermore, unlike Blaze, which allows the grantee to divulge the private key of the grantor from the transformed encrypted data file, a third variable is incorporated into the proxy key to mask the grantee's private key to establish the aforementioned non-commutative or "one-way" property of the transformation.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
April 8, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100